0.1 Problems to try before some fixed day

Problem 0.1.1 (Thue's note) : Let p be prime number, prove that there exists x, y such that $p = 2x^2 + 3y^3$ iff $p \equiv 5, 11 \pmod{24}$.

Problem 0.1.2 (Thue's Note) : Let S be a set of all positive integers which can be represented as $a^2 + 5b^2$ for some coprime integers a, b. Let p be a prime number such that $p = 4n + 3$ for some integer n. Show that if for some positive integer k the numberk p is in S, then $2p$ is in S as well.

0.1.1 Projective Constructions

Construction 1 (Second Intersection of Line with Conic) — Given four points A, B, C, D, no three collinear, and a point P on a line l passing through at most one of the four points, construct the point $P' \in l$ such that A, B, C, D, P, P' line on the same conic.

> ***Solution.*** Let $AP \cap BC = X$, $l \cap CD = Y$, $XY \cap AD = Z$. Then by Pascal's Hexagrummum Mysticum Theorem, we have, $P' = BZ \cap l$

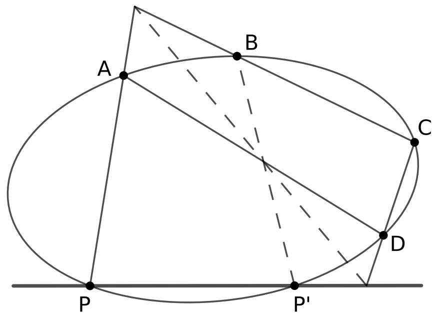

Figure 0.1

Construction 2 (Conic touching conic) — Given a conic $\mathcal{C}$, and two points A, B on it, and C inside of it. Construct the conic $\mathcal{H}$ that is tangent to $\mathcal{C}$ at A, B and passes through C.

> ***Solution.*** Draw the two tangest at A, B which meet at X. Take an arbitrary line passing through X that intersects AC, BC at Y, Z. Take $D = BY \cap AZ$. Then D lies on $\mathcal{H}$ by Pascal. Construct another point E similarly and draw the conic.

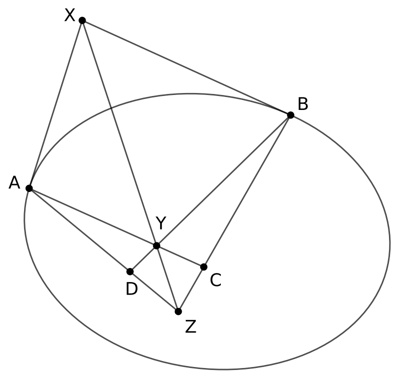

Figure 0.2

Construction 3 (Inconic of a quadrilateral) — Given a convex quadrilateral $ABCD$. $P = AC \cap BD$, $S \in AD, T \in BC$ such that S, P, T are collinear. Construct the conic that touches AB, CD, and also touches AD, BC at S, T respectively.

> ***Solution*** [the_Construction]. Draw the polar line l of P wrt to the quadrilateral. Let $Z = BC \cap l$. Let $ZS \cap AB = U$, $ZT \cap CD = V$. Then $SSUUTTVV$ is our desired conic.

Proof. If $U, V \in CD, AB$ such that UV passes through P, and if the conic passing through U, V and tangent to AD, BC at S, T intersects CD at U' again, then $SV, U'T, DB$ are concurrent. So to show our construction works, we just need to prove that U, V, P are collinear.

Since Pascal's theorem works on $SVBTUD$, we know S, V, B, T, U, D lie on a conic $\mathcal{H}$ and l is the pole of P wrt $\mathcal{H}$. Now, applying Pascal's theorem on $TDVUBS$, and quadrilateral theorem on $BTUD$ and $BVSD$, we have, $ST \cap UV \in AC$, which is P. So we are done.

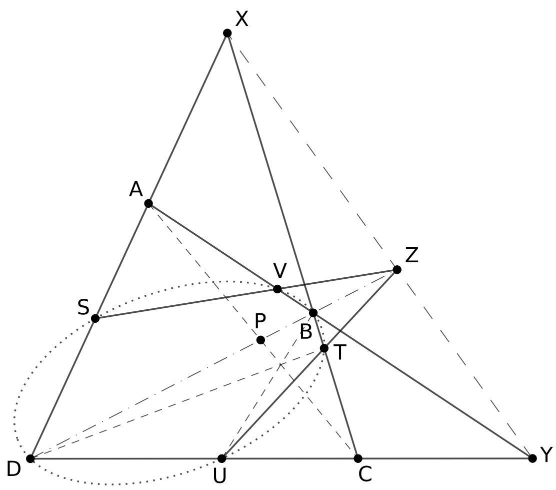

Figure 0.3

Construction 4 (Sharygin Olympiad 2010) — A conic $\mathcal{C}$ passing through the vertices of $\triangle ABC$ is drawn, and three points A', B', C' on its sides BC, CA, AB are chosen. Then the original triangle is erased. Prove that the original triangle can be constructed iff AA', BB', CC' are concurrent.

Solution [the_Construction]**.** Draw $B'C'$. It intersects the circle at X_1, X_2. Draw the conic $\mathcal{H}$ that is tangent to $\mathcal{C}$ at X_1, X_2 and passes through A'. Then BC is tangent to $\mathcal{H}$ at A'.

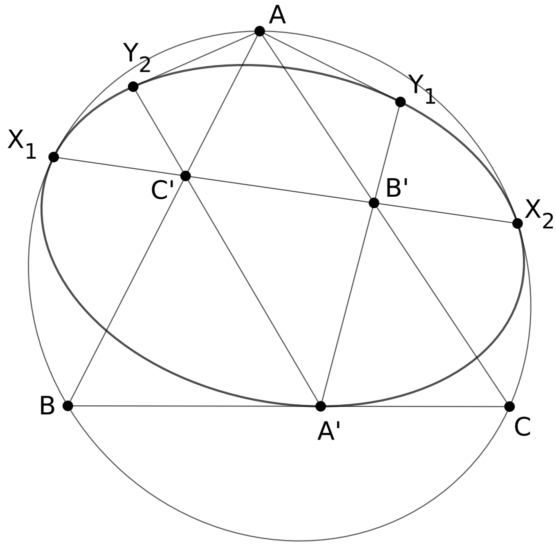

Figure 0.4

Proof. The only if part is easy to prove. Becase if AA', BB', CC' aren't concurrent, then we can get multiple triangles ABC. So suppose that they are concurrent.

Now we define some intersetion points.

$$\begin{array}{rcccc} W_1 & = & BB' & \cap & \mathcal{C} \\ S & = & X_1X_1 & \cap & AW_1 \\ T & = & X_1B & \cap & AX_2 \\ U & = & X_1X_1 & \cap & BC \\ V & = & X_2X_2 & \cap & BC \\ R & = & X_2X_2 & \cap & AW_1 \\ Y_1 & = & A'B' & \cap & SR \end{array}$$

T, S, B' are collinear by Pascal's theorem on $BX_1X_1X_2AW_1$. T, B', V are similarly collinear for $AX_2X_2X_1BC$. And similarly R, B', U are collinear.

We will prove that $\mathcal{H}$ is an inconic of $SRVU$ that goes through A', X_1, X_2.

For a point X on UV, define $f : UV \to UV$ such that $f(X)$ is the second intersection of the conic $X_1X_1X_2X_2X$ ($X_1X_1 = SU, X_2X_2 = RV$) with UV. f is an involution by **??**.

Suppose A_1 is the intersection with the inconic of $SRUV$ through X_1, X_2 and UV. Let $A_2 = X_1X_2 \cap UV$. Then $f(A_1) = A_1, f(A_2) = A_2, f(B) = C$.

Which means, $A(B, C; A_1, A_2) = -1$. Which means $A_1 = A'$. So, $X_1X_2A'X_2X_2$ is an inconic of $SRVU$, just as we wanted.

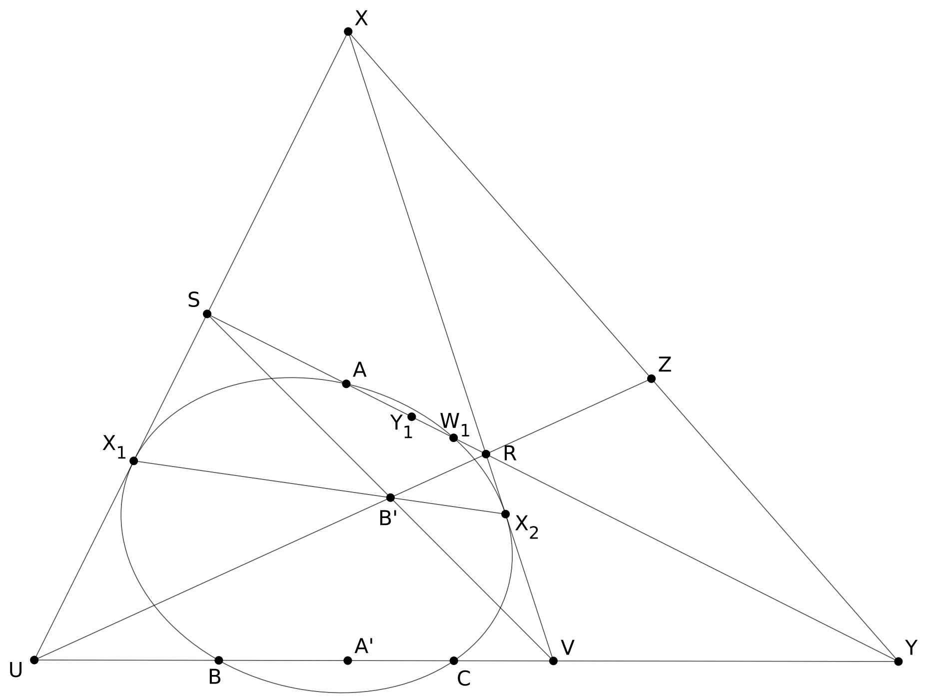

Figure 0.5

Construction 5 (Focus and Directrix of a Parabola) — First draw two parallel segments on the parabola, join their midpoints to get the line parallel to the axis. Then draw the main axis and find out the tip of the parabola. Then draw $f(x) = \frac{x}{2}$ line through P. And find the foot of the intersection of it with the parabola. It is the focus.

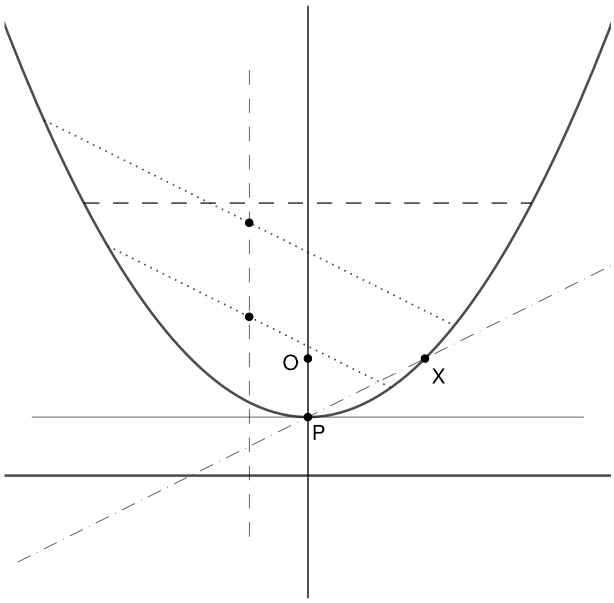

Figure 0.6

0.2 Modular Arithmatic

Theorem 0.2.1 (Thue's Lemma) — Let $n > 1$ be an integer and a be an integer co-prime to n. Then there are integers x, y with $0 < |x|, |y| < \sqrt{n}$ so that

$$x \equiv ay \pmod{n}$$

Such a solution (x, y) is called a "small solution" sometimes.

Proof. Let $r = \lfloor \sqrt{n} \rfloor$ i.e. r is the unique integer for which $r^2 \leq n < (r+1)^2$ The number of pairs (x, y) so that $0 \leq x, y \leq r$ is $(r+1)^2$ which is greater than n. Then there must be two different pairs (x_1, y_1) and (x_2, y_2) so that

$$\begin{aligned} x_1 - ay_1 &\equiv x_2 - ay_2 \pmod{n} \\ x_1 - x_2 &\equiv a(y_1 - y_2) \pmod{n} \end{aligned}$$

Let $x = x_1 - x_2$ and $y = y_1 - y_2$, and we get $x \equiv ay \pmod{n}$. Now, we need to show that $0 < |x|, |y| < r$ and $x, y \neq 0$. Certainly, if one of x, y is zero, the other is zero as well. If both x and y are zero, that would mean that two pairs (x_1, y_1) and (x_2, y_2) are actually same. That is not the case, and so both x, y can not be 0. Therefore, none of x or y is 0, and we are done.

Theorem 0.2.2 (Generalization of Thue's Lemma) — Let α and β are two real numbers so that $\alpha\beta \geq p$. Then for an integer x, there are integers a, b with $0 < |a| < \alpha$ and $0 < |b| < \beta$ so that

$$a \equiv xb \pmod{p}$$

And we can even make this lemma a two dimensional one.

Theorem 0.2.1 (Fermat's 4n+1 Theorem) — Every prime of the form $4n + 1$ can be written as the sum of squares of two coprime integers.

Proof. We know that there is an x such that

$$x^2 \equiv -1 \pmod{p}$$

And by Theorem 0.2.1, there are a, b with $0 < |a|, |b| < \sqrt{n}$ for which

$$\begin{aligned} a &\equiv xb \pmod{p} \\ a^2 &\equiv x^2 b^2 \pmod{p} \\ a^2 + b^2 &\equiv 0 \pmod{p} \end{aligned}$$

Since $a^2 + b^2 < 2p$, we are done.

Theorem 0.2.3 (General Fermat's 4n+1 Theorem) — Let $n \in \{1, 2, 3\}$. If $-n$ is a quadratic residue modulo p, then there exists a, b such that $a^2 + nb^2 = p$

Theorem 0.2.2 (Factors are of the same form) — If $D \in \{1, 2, 3\}$ and $n = x^2 + Dy^2$ for some $x \perp y$, then all of the factors of n are of the form $a^2 + Db^2$.

Proof. This is because the product of two numbers of such form is the same form as them:

$$\begin{aligned}\left(a^2 + Db^2\right)\left(c^2 + Dd^2\right) &= (ac - Dbd)^2 + D(ad + bc)^2 \\ &= (ac + Dbd)^2 + D(ad - bc)^2\end{aligned}$$

And by Theorem 0.2.3 the prime factors of n are of the same form. And so all factors of n are of the same form.

Theorem 0.2.3 (Quadratic Residue -3) — -3 is a quadratic residue of modulo p iff p is of the form $3k + 1$.